Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Distribution of the Ternary Linear Homogeneous Substitutions in a Galois Field into Complete Sets of Conjugate Substitutions.

BY L. E. DICKSON.

The substitutions of the general linear homogeneous group G_m on m indices with coefficients in the $GF[p^n]$ may be classified into complete sets of conjugate substitutions by applying the general theorems given in an earlier paper (*American Journal*, vol. XXII, pp. 121–137). The classification is based upon the canonical forms of the substitutions of G_m. The former depend upon the characteristic determinants of the substitutions (α_{ij}), viz.:

$$\Delta(\lambda) \equiv \begin{vmatrix} \alpha_{11}-\lambda & \alpha_{12} & \cdots\cdots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22}-\lambda & \cdots\cdots & \alpha_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{m1} & \alpha_{m2} & \cdots\cdots & \alpha_{mm}-\lambda \end{vmatrix}$$
$$\equiv (-1)^m (\lambda^m - \alpha_1 \lambda^{m-1} - \alpha_2 \lambda^{m-2} \cdots\cdots - \alpha_m).$$

Furthermore, G_m contains a substitution in whose characteristic determinant the coefficients $\alpha_1, \alpha_2, \ldots\ldots, \alpha_m$ are arbitrary marks of the $GF[p^n]$ such that $\alpha_m \neq 0$. The required substitution is

$$(\alpha_{ij}) \equiv \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \cdots\cdots & \alpha_{m-1} & \alpha_m \\ 1 & 0 & 0 \cdots\cdots & 0 & 0 \\ 0 & 1 & 0 \cdots\cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 \cdots\cdots & 1 & 0 \end{pmatrix}.$$

The present note considers the case $m = 3$. In the article following this, Mr. Putnam treats the case $m = 4$.

Every ternary linear homogeneous substitution in the $GF[p^n]$ can be reduced by a linear ternary transformation of indices (not necessarily with coefficients in the same field) to one of the following five types of canonical forms:

$$\begin{array}{llll}
\mathrm{A}: & x' = \lambda x, & y' = \lambda^{p^n} y, & z' = \lambda^{p^{2n}} z, \\
\mathrm{B}: & x' = \mu x, & y' = \mu^{p^n} y, & z' = \alpha z, \\
\mathrm{C}: & x' = \alpha x, & y' = \beta y\ , & z' = \gamma z, \\
\mathrm{D}: & x' = \alpha x, & y' = \beta y\ , & z' = \beta (z + y), \\
\mathrm{E}: & x' = \alpha x, & y' = \alpha (y + x), & z' = \alpha (z + y),
\end{array}$$

where λ satisfies a cubic equation and μ a quadratic equation, each belonging to and irreducible in the $GF[p^n]$, while α, β, γ denote marks $\neq 0$ of the $GF[p^n]$.

Type A includes $\frac{1}{3}(p^{3n} - p^n)$ distinct sets of conjugate substitutions, those in different sets being not conjugate under G_3. In fact, if we replace λ by λ^{p^n} or by $\lambda^{p^{2n}}$, we obtain from A a substitution conjugate with A under G_3. Any other replacement of λ leads to a substitution not conjugate with A, since its characteristic determinant differs from that of A. Let S be a substitution of G_3 having the canonical form A, where λ is a definite mark of the $GF[p^{3n}]$ not in the $GF[p^n]$. If a substitution T of G_3 be commutative with S, and if we apply to T the same transformation of indices which reduces S to the form A, then T must take the form

$$x' = \sigma^r x, \quad y' = \sigma^{rp^n} y, \quad z' = \sigma^{rp^{2n}} z,$$

where σ is a primitive root of the $GF[p^{3n}]$ and r is some positive integer $\leqq p^{3n} - 1$. Hence, S is commutative with exactly $p^{3n} - 1$ substitutions of G_3, so that S is one of $N \div (p^{3n} - 1)$ conjugate substitutions within G_3, the latter having the order

$$N \equiv (p^{3n} - 1)(p^{3n} - p^n)(p^{3n} - p^{2n}).$$

The number of substitutions of G_3 reducible to the types A is, therefore,

$$\tfrac{1}{3}(p^{3n} - p^n)(p^{3n} - p^n)(p^{3n} - p^{2n}). \tag{a}$$

Type B includes $\frac{1}{2}(p^{2n} - p^n)(p^n - 1)$ distinct sets of conjugate substitutions. In fact, the replacement of μ by μ^{p^n} leads to a conjugate substitution, while any other replacement of μ or any change in α leads to a substitution not conjugate with B. A substitution of G_3 commutative with a particular substitution reducible to a type B has the canonical form

$$x' = \rho^r x, \quad y' = \rho^{rp^n} y, \quad z' = \delta z,$$

where ρ is a primitive root of the $GF[p^{2n}]$ and δ belongs to the $GF[p^n]$ and r is a positive integer $\leqq p^{2n} - 1$. The number of such substitutions is $(p^{2n} - 1)(p^n - 1)$. Hence, the total number of substitutions of G_3 reducible to the canonical forms B is

$$\tfrac{1}{2}(p^{2n} - p^n)(p^n - 1)(p^{3n} - 1)p^{3n}. \tag{b}$$

Type C includes $p^n - 1$ canonical forms with $\alpha = \beta = \gamma$; $(p^n - 1)(p^n - 2)$ canonical forms with $\alpha = \beta \neq \gamma$; a like number with $\alpha = \gamma \neq \beta$; a like number with $\beta = \gamma \neq \alpha$; $(p^n - 1)(p^n - 2)(p^n - 3)$ canonical forms with α, β, γ all distinct. By a suitable transformation of indices, the multipliers α, β, γ in C are permuted in an arbitrary manner. The distinct sets of conjugate canonical substitutions C are, therefore, given by the table:

$p^n - 1$ of type C_1 with $\alpha = \beta = \gamma$;
$(p^n - 1)(p^n - 2)$ of type C_2 with only two equal multipliers, say $\alpha = \beta \neq \gamma$;
$\frac{1}{6}(p^n - 1)(p^n - 2)(p^n - 3)$ of type C_3 with α, β, γ all different.

The most general substitution of G_3 commutative with C_3 is

$$x' = ax, \quad y' = by, \quad z' = cz,$$

so that C_3 is one of $N \div (p^n - 1)^3$ conjugate substitutions within G_3. The most general substitution of G_3 commutative with C_2 is

$$x' = ax + by, \quad y' = cx + dy, \quad z' = ez,$$

so that C_2 is one of $N \div (p^{2n} - 1)(p^{2n} - p^n)(p^n - 1)$ conjugate substitutions. Finally, C_1 is commutative with every substitution of G_3 and is, therefore, conjugate only with itself. The total number of substitutions of G_3 reducible to the canonical forms C is thus:

$$(p^n - 1) + (p^{3n} - 1)(p^n - 2)p^{2n} + \tfrac{1}{6}(p^n - 2)(p^n - 3)(p^{3n} - 1)(p^n + 1)p^{3n}. \tag{c}$$

Type D includes $p^n - 1$ substitutions with $\alpha = \beta$ and $(p^n - 1)(p^n - 2)$ with $\alpha \neq \beta$, no two being conjugate under G_3.

A substitution D with $\alpha = \beta$ is commutative only with the $p^{3n}(p^n - 1)^2$ substitutions of G_3

$$x' = dy + ex, \quad y' = ay, \quad z' = by + az + cx.$$

A substitution D with $\alpha \neq \beta$ is commutative only with the $p^n(p^n-1)^2$ substitutions of G_3

$$x' = ex, \quad y' = ay, \quad z' = by + az.$$

The number of substitutions of G_3 reducible to the types D is thus:

$$(p^n-1)(p^{3n}-1)(p^n+1) + (p^n-1)(p^n-2)(p^{3n}-1)(p^n+1)\,p^{2n}. \qquad \text{(d)}$$

Type E includes $p^n - 1$ substitutions, no two of which are conjugate under G_3. Each is commutative only with the $p^{2n}(p^n-1)$ substitutions of G_3,

$$x' = ax, \quad y' = bx + ay, \quad z' = cx + by + az.$$

The number of substitutions reducible to the types E is thus:

$$(p^n-1)(p^{3n}-1)(p^{2n}-1)\,p^n. \qquad \text{(e)}$$

A check upon the above enumeration of the substitutions G_3 consists in verifying that the sum of the numbers (a), (b), (c), (d), (e) equals the order N of G_3.

THE UNIVERSITY OF TEXAS, *May*, 1900.